UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/086,029	02/27/2002	Nancy Cam-Winget	ATH-0073	3975

30547 7590 06/13/2007
BEVER HOFFMAN & HARMS, LLP
2099 GATEWAY PLACE
SUITE 320
SAN JOSE, CA 95110

EXAMINER	
ZIA, SYED	
ART UNIT	**PAPER NUMBER**
2131	
MAIL DATE	**DELIVERY MODE**
06/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/086,029	**Applicant(s)** CAM-WINGET ET AL.	
	Examiner Syed Zia	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04/02/2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on April 02, 2007. Original application contained Claims 1-41. Applicant currently amended Claims 9, 13, 18, 21, 27-34, and 40-41. Applicant amendments filed on April 02, 2007 have been entered and made of record. Therefore, presently pending claims are 1-41.

Response to Arguments

Applicant's arguments filed April 02, 2007 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1-41 applicants argued that in the system of cited prior art (CPA) [Gray et al. U. S. Patent 5,706,348] does not *"MAC sub-layer that initiates derivation of a new key encryption"*.

This is not found persuasive. The system of cited prior art clearly discloses a encrypted communication system, wherein the key synchronization system store needed encryption keys and perform other operations required to assure synchronization of encryption and decryption keys in active use at source and destination systems. The source node will further include a packet transmission component for transmitting ATM cells after the data payloads in the cells are encrypted using the current encryption key. A destination node also include a packet receiving system 48 for receiving ATM cells from the wide area network, a decryption controller 50 for decrypting the data payload of each cell and a key synchronization system 54 for making sure that the decryption key used for a particular ATM cell corresponds to the encryption key used in encrypting that same cell (col.3 line 48 to col.7 line 46).

Therefore, the system of cited prior art describes a system and method for refreshing a key and indicating when the refreshed key is to be invoked.

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. The examiner is not trying to interpret the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that the system of cited prior arts does teach or suggest the subject matter broadly recited in independent Claim 3 and in subsequent dependent Claims. Accordingly, rejections for claims 1-41 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1-41 rejected under 35 U.S.C. 102(b) as being anticipated by Gray et al. U. S. Patent 5,706,348.

2. Regarding Claim 1, Gray teach and describe a method for encrypted communications between a first transceiver and a second transceiver, the method comprising:
sending from a first transceiver to a second transceiver a request to initiate derivation of a new encryption key, the request to initiate a new encryption key derivation being controlled by a MAC sub-layer and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets (col.3 line 48 to col.5 line 39).

3. Regarding Claim 26, Gray teach and describe a first transceiver that is to conduct encrypted communications with a second transceiver, the first transceiver comprising: a physical control layer that sends to the second transceiver a request to initiate derivation of a new encryption key, the request to initiate a new encryption key derivation being controlled by a MAC sub-layer and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets (col.3 line 48 to col.5 line 39).

4. Regarding Claim 37,Gray teach and describe a first transceiver that is to conduct encrypted communications with a second transceiver, the first transceiver comprising: a physical control layer that receives from the second transceiver a request to initiate derivation of a new encryption key, the request to initiate a new encryption key derivation being controlled by a

MAC sub-layer and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets, and a first nonce needed to derive the new encryption key (col.3 line 48 to col.5 line 39).

5. Claims 2-7, 10, 12, 14-15, 18, 27-34, 36, and 38-40are rejected applied as above rejecting Claims 1, 26, and 37. Furthermore,

As per claim 2-5, wherein the exchange threshold is: a time, a counter value, a number of packets, at least one of a time, a counter value, and a number of packets (col. 3 line 48 to col.4 line 40).

As per claim 6, wherein the request to initiate derivation of the new encryption key includes a timeout limit that indicates that a session is to be at least one of aborted or retried when the timeout limit is satisfied (col. 3 line 48 to col.4 line 40).

As per claim 7, wherein the request to initiate derivation of the new encryption key is sent from the first transceiver to the second transceiver and the new encryption key is to be generated at the second transceiver, in response to the request, before a key space of an old nonce value has been exhausted (col. 5 line 56 to col.6 line 8).

As per claim 8, wherein the request to initiate derivation of the new encryption key includes a first nonce needed to derive the new encryption key (col. 5 line 40 to line 48).

As per claim 10, wherein the request to initiate derivation of the new encryption key includes a first transceiver authentication indication that authenticates the first transceiver to the second transceiver (col. 5 line 56 to col.6 line 8).

As per claim 12, wherein the request to initiate derivation of the new encryption key includes a new initial nonce value that is used along with the new encryption key for encryption (col.6 line 55 to col.7 line 46).

As per claim 14, further comprising: determining whether the new encryption key needs to be derived; and wherein sending the request to initiate derivation of the new encryption key is based upon the determination of whether the new encryption key needs to be derived (col.6 line 55 to col.7 line 46).

As per claim 15, further comprising: generating the new encryption key at the first transceiver and the second transceiver; determining at least one of the first transceiver and the second transceiver whether the exchange threshold has been satisfied; and encrypting at least one of the first transceiver and the second transceiver using the new encryption key when the exchange threshold has been satisfied (col.4 line 60 to col.5 line 40).

As per claim 18, wherein the request to initiate derivation of the new encryption key includes a first nonce needed to derive the new encryption key, the method further comprising: sending from the second transceiver to the first transceiver, in response to the request to initiate derivation of the new encryption key, a second nonce needed to derive the new encryption key (col. 4 line 41 to col.5 line 39).

As per claim 27, wherein the exchange threshold is a number of packets (col. 3 line 48 to col.4 line 40).

As per claim 28-30, wherein: the request includes a first transceiver identifier that authenticates the first transceiver to the second transceiver, the request to initiate derivation of the new encryption key includes a timeout limit that indicates that a session is to be at least one of aborted or retried when the timeout limit is satisfied, the request to initiate derivation of the new encryption key includes a first nonce needed to derive the new encryption key (col. 4 line 41 to col.5 line 39).

As per claim 31, wherein the request to initiate derivation of the new encryption key includes a first transceiver authentication indication that authenticates the first transceiver to the second transceiver (col. 4 line 41 to col.5 line 39).

As per claim 32, wherein the request to initiate derivation of the new encryption key includes a new initial nonce value that is used in combination with the new encryption key for encryption (col. 5 line 14 to line 39).

As per claim 33, wherein the physical control layer determines whether the new encryption key needs to be derived before sending the request to initiate derivation of the new encryption key; and wherein sending the request to initiate derivation of the new encryption key is based upon the determination of whether the new encryption key needs to be derived (col. 4 line 41 to col.5 line 39).

As per claim 34, wherein the physical layer receives a second nonce from the second transceiver, generates the new encryption key, determines whether the exchange threshold has been satisfied, and encrypts using the new encryption key when the exchange threshold has been satisfied (col. 4 line 41 to col.5 line 39).

As per claim 36, wherein the physical control layer sends the request early enough so that the new encryption key is to be generated at the second transceiver, in response to the request, before a key space of an old nonce value has been exhausted (col. 4 line 41 to col.5 line 39).

As per claim 38, wherein the physical control layer sends to the second transceiver, in response to the request to initiate derivation of the new encryption key, a second nonce (col. 4 line 60 to col.5 line 39).

As per claim 39, wherein the physical control layer sends to the second transceiver, in response to the request to initiate derivation of the new encryption key, a status indication indicative of the first transceiver's determination of the feasibility of being able to commence using the new encryption key at the first transceiver in accordance with the exchange threshold (col. 4 line 60 to col.5 line 39).

As per claim 40, wherein the physical control layer generates the new encryption key determines whether the exchange threshold has been satisfied, and encrypts using the new encryption key when the exchange threshold has been satisfied (col. 3 line 40 to col.5 line 39).

6. Claims 9, 11, 13, 16, 19, and 35 are rejected applied as above rejecting Claims 8, 10, 12, 15, 18, and 34. Furthermore

As per claim 9, further comprising: sending from the second transceiver to the first transceiver, in response to the request to initiate derivation of the new encryption key, a second nonce needed to derive the new encryption key (col. 4 line 41 to col.5 line 39).

As per claim 11, further comprising sending from the second transceiver to the first transceiver, in response to the request to initiate derivation of the new encryption key, a second transceiver authentication indication which authenticates the second transceiver to the first transceiver (col. 4 line 41 to col.5 line 39).

As per claim 13, further comprising: sending from the second transceiver, in response to the request to initiate derivation of the new encryption key, a status indication indicative of the second transceiver's determination of the feasibility of being able to commence using the new encryption key at the second transceiver in accordance with the exchange threshold (col. 4 line 41 to col.5 line 39).

As per claim 16 further comprising: continuing communication between the first transceiver and the second transceiver using for encryption an old encryption key generated before the new encryption key when the exchange threshold has still not been satisfied (col. 4 line 41 to col.5 line 39).

As per claim 19, further comprising: generating at least one of the first transceiver and the second transceiver the new encryption key; determining at least one of the first transceiver and the second transceiver whether the exchange threshold has been satisfied; and encrypting at least one of the first transceiver and the second transceiver using the new encryption key when the exchange threshold has been satisfied (col. 4 line 60 to col.5 line 39).

As per claim 35, wherein the physical control layer continues using for encryption an old encryption key generated before the new encryption key when the exchange threshold has still not been satisfied (col. 3 line 40 to col.5 line 39).

As per claim 38, wherein the physical control layer sends to the second transceiver, in response to the request to initiate derivation of the new encryption key, a second nonce (col.4 line 41 to col.5 line 39).

As per claim 39, wherein the physical control layer sends to the second transceiver, in response to the request to initiate derivation of the new encryption key, a status indication indicative of the first transceiver's determination of the feasibility of being able to commence using the new encryption key at the first transceiver in accordance with the exchange threshold (col. 3 line 40 to col.5 line 39).

As per claim 41, wherein the physical control layer continues communication between the first transceiver and the second transceiver using for encryption an old encryption key generated before the new encryption key when the exchange threshold has still not been satisfied (col. 3 line 40 to col.5 line 39).

6. Claims 17, 20-25 are rejected applied as above rejecting Claims 16, 19. Furthermore

As per claim 17, wherein encrypting using the new encryption key occurs without disrupting communication between the first transceiver and the second transceiver (col. 4 line 41 to col.5 line 39).

As per claim 20, wherein the request to initiate derivation of the new encryption key includes a new initial nonce value and encrypting includes using the initial nonce value and the new encryption key for encryption, the method further comprising: determining whether the new encryption key needs to be derived; and wherein sending the request to initiate derivation of the new encryption key is based upon the determination of whether the new encryption key needs to be derived (col. 4 line 41 to col.5 line 39).

As per claim 21, the method comprising: sending from first receiver to the second transceiver a first transceiver authentication indication that authenticates the first transceiver to the second transceiver; and sending from the second transceiver to the first transceiver a second transceiver authentication indication that authenticates the second transceiver to the first transceiver (col. 4 line 41 to col.5 line 39, and col.5 line 65 to col.6 line 8)).

As per claim 22, further comprising sending from the first transceiver to the second transceiver the second nonce (col. 4 line 41 to col.5 line 39).

As per claim 23 further comprising: continuing communication between the first transceiver and the second transceiver using an old encryption key generated before the new encryption key when the exchange threshold has still not been satisfied (col. 4 line 41 to col.5 line 39, and col.5 line 65 to col.6 line 8).

As per claim 24, wherein encrypting using the new encryption key occurs without disrupting communication between the first transceiver and the second transceiver col. 4 line 41 to col.5 line 39).

As per claim 25, wherein the request to initiate derivation of the new encryption key includes a timeout limit that indicates that a communication is one of aborted and retried when the timeout limit is satisfied (col. 4 line 41 to col.5 line 39).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
June 08, 2007

06/15/2007
SYED ZIA
PRIMARY EXAMINER
AU 2131